REMARKS

In the Office Action mailed March 18, 2003 the Examiner noted that claims 1-26 were pending and rejected all claims. Claims 1-6, 12, 13, 15-19, 22-24 and 26 have been amended and, thus, in view of the forgoing claims 1-10, 12-19 and 22-26 remain pending for reconsideration which is requested. No new matter has been added. The Examiner's rejections are traversed below.

In the Office Action the Examiner rejected claims 2, 22 and 26 under 35 U.S.C. section 112 paragraph 2 as indefinite. The claims have been amended in consideration of the Examiner's comments and it is submitted they satisfy the requirements of the statute. If additional concerns with the claims arise, the Examiner is invited to telephone to resolve the same. Suggestions by the Examiner are also welcome. Withdrawal of the rejection is requested.

On pages 5, 6, 7 and 10 of the Office Action the Examiner rejected all claims either under 35 U.S.C. § 102 as anticipated by Kuroda or under 35 U.S.C. § 103 as obvious over Kuroda and Mittra.

The present invention is designed to improve security by using a plurality of encryption keys for securing electronic data where a different type of key is used depending on particular usage, such as data storage, data communication, etc. This objective differs from that of Kuroda. It is an object of Kuroda to guarantee the genuineness of electronic data (prevent illegal alteration and insure source reliability) to maintain/certify legal aspects (evidence) of the electronic data. The object of Mittra is also different from that of the present invention. The objective of Mittra is to secure a multicast communication inside/outside a secure group. This is more limited and different from the object of the present invention as discussed above, which covers not only communication, but also storage.

In an effort to solve the different problems of the present invention, Kuroda and Mittra, they all behave differently. In the present invention, the electronic data itself is encrypted to secure the data. In Kuroda, a variety of authentication type information is encrypted to guarantee the genuineness of the electronic data. Mittra, which targets only communication, is limited to the distribution of keys for communication. The present invention distributes individual keys for storage purposes while common keys are distributed for communication.

When the present invention of claims 1-23 and Kuroda are compared, they fundamentally differ in their methods of using keys. As set forth in claim 1, in the present invention, electronic data stored in a storage apparatus, to which the key management means belongs, is encrypted using an individual key, and data that is transmitted to and received from other storage apparatuses is encrypted or authenticated using a common key.

However, in Kuroda, an individual key is only used to generate various certificates, and is not used to encrypt electronic data. A common key is used not only to encrypt electronic data, but also to generate authentication information. Specifically, a transaction identifier is generated using a file identifier, an identifier is generated using a file identifier, an identifier for a storage apparatus, time, an identifier for opposite storage apparatus, etc., and the transaction identifier is combined with electronic data. Authentication information is generated using a common key.

For example, as shown in Fig. 11 of Kuroda, an individual key 25a is used when a data transfer request certificate 26 is generated in a storage apparatus A20a, and authentication information 23 for electronic data is generated using a master (common) key.

When the electronic data is received by a storage apparatus B20b, the contents of the authentication information is authenticated using a master key, and the electronic data is stored together with the data transfer request certificate 26. Then, a storage certificate 27 is generated using an individual key 25b and is transmitted to the storage apparatus A20a.

With respect to the data transfer request certificate, Kuroda simply discloses that the data transfer request certificate is stored together with electronic data and does not disclose its authentication at all.

In Mittra, a trusted intermediary (TI), shown in Figs. 1 - 3, is similar to the lower-order group master in a higher-order group, which is positioned with respect to a lower-order group, shown in Fig. 16 of the present invention. In the present invention, for example, a group in the original claim 2 corresponds to groups 1 and 2. As noted by the Examiner, Mittra uses the TI to generate and distribute a common key.

In addition to the differences in use of the keys over Kuroda discussed above, in the present invention, a group master ("main electronic data storage") in each group generates and distributes an individual key for each storage apparatus in the group (see particularly claims 1, 15-17, 22 and 23). This is also not found/suggested in Kuroda and/or Mittra.

For the above-discussed reasons, it is submitted that claims 1-23 are patentably distinct over the prior art.

Another feature of the present invention as compared to the prior art is the uniqueness of the individual key (see claim 24). As noted above, Kuroda is directed to a system that includes master keys and individual keys. The master keys are used among the plurality of electronic data storage apparatuses and are particularly called common keys (see, for example, col. 4, lines 8- 10 and col. 23, lines 31-32). Kuroda discusses the individual keys in two versions that, as will be shown below, are not particularly relevant to the present invention. In the first version, Kuroda describes the individual key as being a shared key that is not unique (see col. 1, lines 20-24 and col. 2, line 20). This individual key is really a common key since it is shared. The second version of the individual key is used by a first apparatus to generate a certificate, as discussed above, to send to a second apparatus and Kuroda states that each key is unique for an apparatus. See col. 7, line 59- col. 9, line 21, and more particularly:

> When electronic data is transferred from the electronic data storage apparatus A20a to the electronic data storage apparatus B20b, the electronic data storage apparatus A20a first generates a data transfer request certificate 26 using the individual key 25a, and a data transfer request certificate 26 is transmitted together with the authentication information data 23 to the electronic data storage apparatus B20b.
> The electronic data storage apparatus B20b verifies the contents of the authentication information, stores the data together with a data transfer request certificate if the electronic data storage apparatus B20b determines that an illegal amendment has not been made to the data, and then generates a storage certificate 27 using the individual key 25b and transmits it to the electronic data storage apparatus A20a.
> The electronic data storage apparatus A20a stores the storage certificate 27, generates a storage certificate receipt certificate 28 using the individual key 25a, and transmits it to the electronic data storage apparatus B20b. The electronic data storage apparatus B20b stores the storage certificate receipt certificate 28, and terminates the process of transferring the electronic data.

(col. 8, lines 40-60).

As noted in the text above, this version of the key associated with or maintained by a first apparatus is used for transmitting a data certificate to and storing data of the first apparatus in a second apparatus. In this context, the Kuroda individual key is not used for storage in the apparatus that maintains the key nor is the key unique to the apparatus (the second apparatus) in which the data is stored as the key originates with the first apparatus. In a certain sense this version of the Kuroda individual key is also a common key since it is used in two different apparatuses.

In contrast, the present invention as recited in claim 24 is directed to data storage in a storage system associated with other data storage systems. The encryption encrypts data to be stored locally in the associated data storage unit or encrypts data that is to be transferred to one of the other data storage systems where it can be stored in one of the other data storage units. The key management manages two types of keys, a common global key and an individual local key. The common key is used to encrypt and decrypt data that is being transferred globally between data storage systems. That is, when a first data storage system is transferring data to or receiving from a second data storage system a common global key is used for the encryption/decryption. The individual key is used to encrypt/decrypt data to be stored locally in the data storage unit associated with the key management unit that manages the individual key. This individual local key is uniquely used by and only associated with the data storage unit, and is used for data storage in the data storage unit only by the data storage system that manages the individual local key (see claim 24).

The present invention teaches something beyond Kuroda. In the context of Kuroda and the present invention, the Kuroda "individual" key would be used to transmit data from a first electronic data storage apparatus to a second apparatus, this data would be encrypted using the individual local key of the second apparatus (something not found in Kuroda) and the newly encrypted data would be stored in the storage unit of the second apparatus. Kuroda does not teach or suggest this.

By having an individual local key only used by the local apparatus that maintains the key and for storage of data within that apparatus, the present invention provides more secure data storage.

Mittra is directed to a system that uses group keys to transmit a message to members of the group essentially simultaneously, called a multicast or broadcast transmission (see, for example, col. 4, lines 6-19). These group keys are common keys. Mittra says nothing about having common global keys and individual local keys, much less individual local keys that are unique to and used only within a particular storage apparatus as is the case in the present invention.

For the above-discussed reasons, it is submitted that claims 24 - 26 are patentably distinct over the prior art.

It is submitted that the invention of independent claims distinguish over the prior art and withdrawal of the rejection is requested.

The dependent claims depend from the above-discussed independent claims and are patentable over the prior art for the reasons discussed above. The dependent claims also recite additional features not taught or suggested by the prior art. For example, claim 4 calls for the individual key to be used to generate a group key. Nothing in the prior art teaches or suggests this. It is submitted that the dependent claims are independently patentable over the prior art.

It is submitted that the claims satisfy the requirements of 35 U.S.C. § 112. It is further submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 6/10/3

By: _____

J. Randall Beckers
Registration No. 30,358

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500